AMENDMENTS TO THE CLAIMS

1. (Currently amended) A system for communicating over a network having a plurality of secured users utilizing multi-level network security devices and a plurality of unsecured users employing no network security devices, said system comprising:

an interface unit configured to send a message from a first user;

a first multi-level network security device configured to:

intercept said message from the first user; and

~~a host configured to~~ discard said message if said message violates security parameters associated with said interface unit,

wherein in a first mode, the first multi-level network security device is configured to send said message to a second user, and

wherein in a second mode, the first multi-level network security device comprises an encryptor configured to encrypt said message and send said encrypted message to a second multi-level network security device, and wherein in said second mode the second multi-level network security device comprises a decryptor configured to decrypt the message and send said decrypted message from said second multi-level network security device to a third user selected from said plurality of secured users.

2. (Original) The system of Claim 1, further comprising a third multi-level network security device configured to intercept said encrypted message, validate a signature of said first multi-level network security interface, and send said encrypted message from said third multi-level network security interface to said second multi-level network security interface.

3. (Original) The system of Claim 1, wherein each multi-level network security device is configured to use association establishment messages for authenticating other multi-level network security interfaces.

4. (Original) The system of Claim 1, wherein each multi-level network security device is configured to use association establishment messages for exchanging security parameters between said multi-level network security interfaces.

5. (Currently Amended) A system for mixed enclave communications over a network having both secured and unsecured users, the system comprising:

a network security device configured to permit communication over the network between one of said secured users and one of said unsecured users, and further configured to dynamically determine whether a user initiating communication is one of said secured users or one of said unsecured users; and

a control module operationally coupled to said network security device, the control module being configured to control passage of information between said one of said secured users and said one of said unsecured users to secure information residing with said one of said secured users against transfer to said one of said unsecured users when not permissible, wherein the network security device is configured to use association establishment messages for said secured users in authenticating each other.

6. (Original) The system of Claim 5, wherein the network security device is configured to examine Internet Protocol (IP) addresses for identifying the secured and unsecured users.

7. (Cancelled).

8. (Original) The system of Claim 5, wherein the network security device is configured to use association establishment messages for the secured users exchanging security parameters.

9. (Original) The system of Claim 5, wherein the network security device comprises an encryptor configured to encrypt information residing with one of the secured users.

10. (Currently amended) An apparatus for providing multi-level security in a computer network having a plurality of users and at least one relatively secure portion relative to at least one relatively unsecure portion of the network, the apparatus comprising:

a network security device configured to intercept a message transmitted between said at least one secure and said at least one unsecure portions of said network, and further configured to determine whether transmission of said intercepted message violates network security parameters ~~will be violated by said intercepted message~~;

an encryptor configured to encrypt said intercepted message if said intercepted message:

~~will not violate said network security parameters,~~

originates from a first secure portion of said network,

is destined for ~~another~~ a second secure portion of said network, and

~~will traverse~~ wherein said computer network is configured so that said intercepted message traverses an unsecure portion of said network to reach said second secure portio of said network; and

if said network security ~~parameters will not be violated~~ device determines that said intercepted message violates said network security parameters:

in a first mode, the network security device is configured to transmit said intercepted message; and,

in a second mode, the network security device is configured to transmit said encrypted intercepted message.

11. (Original) The apparatus Claim 10, wherein the network security device is further configured to select the types of messages that are permissible.

12. (Original) The apparatus of Claim 10, wherein the network security device is further configured to examine Internet protocol (IP) addresses for identifying the source and destination of said message.

13. (Original) The apparatus of Claim 12, wherein the network security device is further configured to use association establishment messages for allowing those users which reside in said at least one secure portion of said network to authenticate other users residing in other secure portions of said network.

14. (Original) The apparatus of Claim 13, wherein said association establishment messages comprise security parameters.

15. (Original) The apparatus of Claim 13, further comprising a host configured to utilize a message intended to evoke a response from a destination user selected from said plurality of users and intended to receive said message to determine whether said destination user resides in the same portion of the network as a source user selected from said plurality which sent said message.

16. (Original) The apparatus of Claim 15, wherein said message intended to evoke a response from said destination user comprises a message which evokes a response only if said destination user and source user reside in the same portion of said network.

17. (Original) The apparatus of Claim 10, further comprising a waiting queue configured to queue passage of information.

18. (Original) The apparatus of Claim 10, wherein the network security device is configured to create an entry in an association table indicative of the source of a received message.

19. (Original) The apparatus of Claim 18, wherein the network security device is configured to compare the message destination's security level to that of the source of said intercepted message, so as to determine if said intercepted message may proceed.

20. (Currently amended) The apparatus of Claim 19, wherein the network security device is configured to release said intercepted message if the message destination's security level is higher than that of the source~~, the intercepted message is permissible to be released~~.

21. (Currently amended) The apparatus of Claim 19, wherein the network security device is configured to communicate the message between the message source and destination if the message destination's security level is equivalent to that of the source~~, information transfers between the message source and destination~~.

22. (Currently amended) The apparatus of Claim 19, wherein the network security device is configured to prohibit release of said message when the message destination's security level is lower than that of the source~~, the intercepted message is not permissible to be released,~~ unless said message is predicted.

23. (Currently amended) An apparatus for communicating over a network having a plurality of secured users utilizing multi-level network security devices and a plurality of unsecured users, the apparatus comprising:

a first network security device configured to control the transmission of a message from a first user to a second user, wherein

in the event that either (a) the first user is a secured user and the second user is an unsecured user, or (b) the first user is an unsecured user and the second user is a secured user, the first network security device is configured to intercept a message sent by the first user, determine whether transmission of said message breaches network security parameters~~will be breached by said message~~, and transmit said message to said second user if transmission of said message does not breach network security parameters~~will not be breached by said message~~, and

in the event that both the first and second users are secured users, the first network security device is configured to

intercept the message sent by the first user,

determine whether transmission of said message breaches network security parameters ~~will be breached by said message~~,

encrypt said message ~~using if network security parameters will not be breached by transmission of said message~~,

transmit said encrypted message to a second network security device utilized by said second user if ~~network security parameters will not be breached by~~ transmission of said message does not breach network security parameters , and

the second network security device is configured to decrypt said encrypted message and transmit said decrypted message to the second user ~~if network security parameters will not be breached by transmission of said message~~.

24. (Original) The apparatus of Claim 23, wherein the first network security device is configured to compare the message destination's security level to that of the source of said intercepted message.

25. (Original) The apparatus of Claim 24, wherein:

when the message destination's security level is higher than that of the source, the intercepted message is permissible to be released;

when the message destination's security level is equivalent to that of the source, information transfers between the source and destination; and,

when the message destination's security level is lower than that of the source, the intercepted message is not permissible to be released, unless said message is predicted.

26. (New) The apparatus of Claim 22, wherein said message is predicted if another message is first received by the source from the destination.

27. (New) The apparatus of Claim 22, wherein said message is predicted if said message responds to another message from the destination.

28. (New) An apparatus for communicating over a network having a plurality of secured users utilizing multi-level network security devices and a plurality of unsecured users, the apparatus comprising:

a multi-level network security device configured to:

intercept a message from a source to a destination;

determine a first security parameter associated with the source;

determine a second security parameter associated with the destination;

identify a security policy based on the first and second security parameter;

determine whether said message complies with said security policy; and

transmit said message to the destination if said message complies with said security policy.

29. (New) The system of Claim 24, wherein the system further comprises an encryptor configured to encrypt said message if so specified by said security policy.

30. (New) The system of Claim 24, wherein the first security parameter identifies the source as one of a secured or unsecured user.

31. (New) The system of Claim 24, wherein the second security parameter identifies the destination as a secured or unsecured user.

32. (New) The system of Claim 24, wherein at least one of the first or second security parameters identifies a classification level of data.

33. (New) The system of Claim 24, wherein the multi-level network security device is configured to inhibit covert channel use.

34. (New) The system of Claim 33, wherein the multi-level network security device is configured to limit the rate of data transfer between a secure source and an insecure destination to a convert channel rate.

35. (New) The system of Claim 24, wherein the multi-level network security device is configured to inhibit denial of service attacks.

36. (New) The system of Claim 24, wherein the multi-level network security device is configured to inhibit denial of service attacks.

37. (New) The system of Claim 24, wherein said multi-level network security device is configured to use association establishment messages for determining at least one of the first or second security parameters.

38. (New) A method for mixed enclave communications over a network including both secured and unsecured users, said method comprising:

permitting communications over the network between one of said secured users and one of said unsecured users;

discovering dynamically by said secured user whether a user initiating communications is one of said secured users or one of said unsecured users;

controlling passage of information between said one of said secured users and said one of said unsecured users for securing given information residing with said one of said secured users against transference to said one of said unsecured users when not permissible; and

inhibiting covert channel use.

39. (New) The method of Claim 38, wherein inhibiting covert channel use comprises limiting the rate of data transfer between a secure source and an insecure destination to a convert channel rate.

40. (New) The method of Claim 38, wherein permitting communication comprises permitting Internet Protocol communications.

41. (New) The method of Claim 40, wherein inhibiting covert channel use comprises detecting dialog sequence errors.

42. (New) The method of Claim 38, wherein discovering includes using Internet Protocol (IP) addresses for identifying the secured and unsecured users.

43. (New) The method of Claim 38, wherein discovering includes using association establishment messages for said secured users authenticating each other.

44. (New) The method of Claim 38, wherein discovering includes using association establishment messages for the secured users exchanging security parameters.

45. (New) The method of Claim 38, wherein for communications between one of the secured users and one of the unsecured users, the secured user employs a waiting queue to influence passage of information.

46. (New) The method of Claim 38, wherein controlling passage of information comprises:

determining when one of the secured users receives initial information from one of the unsecured users that is not already established; and

creating an entry in an association table indicative of at least the unsecured user's IP address and association type.

47. (New) The method of Claim 46, wherein controlling passage of information comprises further comparing a security level of the one of the secured users to that of the unsecured user for determining if information to the unsecured user can be allowed to proceed.

48. (New) A method for mixed enclave communications over a network including both secured and unsecured users, said method comprising:

permitting communications over the network between one of said secured users and one of said unsecured users;

discovering dynamically by said secured user whether a user initiating communications is one of said secured users or one of said unsecured users;

controlling passage of information between said one of said secured users and said one of said unsecured users for securing given information residing with said one of said secured users against transference to said one of said unsecured users when not permissible; and

inhibiting denial of service attacks.

49. (New) The method of Claim 48, wherein inhibiting denial of service attacks comprises detecting lack of activity on a machine associated with one of said secured or unsecured users and blocking communications from said machine.

50. (New) The method of Claim 48, wherein inhibiting denial of service attacks comprises detecting data corruption exceeding a predetermined threshold in communications from one of said secured or unsecured users and blocking communications from said user.

51. (New) The method of Claim 48, wherein inhibiting denial of service attacks comprises detecting unauthorized access by one of said secured or unsecured users and blocking communications from said one of said secured and unsecured users.

52. (New) The method of Claim 48, wherein permitting communication comprises permitting Internet Protocol communications.

53. (New) The method of Claim 48, wherein discovering includes using Internet Protocol (IP) addresses for identifying the secured and unsecured users.

54. (New) The method of Claim 48, wherein discovering includes using association establishment messages for said secured users authenticating each other.

55. (New) The method of Claim 48, wherein discovering includes using association establishment messages for the secured users exchanging security parameters.

56. (New) The method of Claim 48, wherein for communications between one of the secured users and one of the unsecured users, the secured user employs a waiting queue to influence passage of information.

57. (New) The method of Claim 48, wherein controlling passage of information comprises:

determining when one of the secured users receives initial information from one of the unsecured users that is not already established; and

creating an entry in an association table indicative of at least the unsecured user's IP address and association type.

58. (New) The method of Claim 57, wherein controlling passage of information comprises further comparing a security level of the one of the secured users to that of the unsecured user for determining if information to the unsecured user can be allowed to proceed.

59. (New) The method of Claim 58, wherein inhibiting denial of service attacks comprises detecting an unauthorized level of the unsecured user and blocking communications from said unsecured user.